Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI-LEVEL TRUST ARCHITECTURE FOR MOBILE ADHOC NETWORKS BASED ON CONTEXT-AWARE

[1] A.RAJESH, [2] DR. N. MOHAN KUMAR

[1]Research Scholar, ANNA University Chennai, India,
[1] Associate Professor / Department of Computer Science and Engineering,
[2] Professor /Department of Electronics and Communication Engineering,
[1,2] S.K.P. Engineering College, [1,2] Thiruvannamalai, [1,2] Tamil Nadu, [1,2] India.
E-mail: [1]svishnuraj7@yahoo.co.in , [2]nmphdju@gmail.com

ABSTRACT

Mobile ad hoc networks (MANETs) are not favorable to centralized trust architecture and literature review provides several security framework and solutions for trust management. However, there is no unified architecture for MANET to exploit deployed security models based on trust. This study presents compelling trust architecture in which a trust based security model is superimposed with three trust models such as a low-level trust model, a medium-level trust model, and a high-level trust model based on context-aware security. The low-level trust model meets the necessary security requirements using direct observations. The medium-level trust model ensures medium security level using direct observations and recommendation messages. The high-level trust model provides a highly secured system with high complexity and computational cost. The proposed work is formulated based on the application context to determine the trust-level in geographic routing protocol. The proposed trust is fully distributed and application context dependent and dynamic in nature. The proposed multi-level trust model is integrated with Position based Opportunistic Routing (POR) Protocol that selects the trusted next hop in the routing path. The correctness of the proposed scheme is analyzed using network simulator (NS-2). Proposed work increases packet deliver ratio and throughput significantly.

Keywords: *Mobile Ad Hoc Networks, Geographical Routing, Trust Management, Context-aware Trust, Trust based Security*

1. INTRODUCTION

MANET has gained more attention due to its salient features like infrastructure less and multi-hop communication. On the other hand, it is susceptible to a highly error prone wireless broadcasting channel, and actively changing network topology. Conventional topology based MANET routing protocols is not efficient with the node's mobility. Route maintenance is usually difficult due to the highly dynamic network topology. Hence, topological routing is not efficient and scalable. The idea of trust is significant to routing protocol developers in which introducing trust relationship among nodes is a challenging task to optimize the network metrics. Trust is defined as a confidence level (relationship) among the nodes that take part in the routing. These relationships are determined based on facts gathered from the history of previous interactions among the nodes. If the interactions are true to the protocol, the value of trust among these nodes will be accumulated. Trust of a node may be represented as a measure of belief over the actions of its neighboring nodes, and also considers the importance of context. The trust value plays a vital role in the routing. In MANET routing protocol, trust values are mainly associated with two events such as trust request and trust recommendation. Each node maintains a trust record related to these two events. The source node may even use the trust record to detect the malicious activities in the routing.

Trust evaluation in topological routing protocol is a taxing job due to the dynamic network topology. Geographical routing does not require any predetermination of the end-to-end route. Therefore, geographical routing is more efficient and scalable. POR is a widely used geographic routing protocol. POR exploits MAC layer feedback that provides another chance to re-route in case of transmission failure [17]. The

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

evaluation of trust in geographical routing is straightforward compared to that of in topological routing. The MANETs are susceptible to security threats due to the network dynamics, de-centralized architecture and broadcasting nature. However, security techniques developed for fixed networks are not suitable for MANETs due to its dynamic characteristics. Trust computation is a crucial factor in the design and analysis of the secure ad hoc routing system.

Trust is a context dependent factor. In MANET, different levels of trust are preferred in routing depending on the application. MANETs are used in several applications such as a military battlefield, collaborative works, and the personal area network (PAN). For instance, routing messages in military applications require a higher level of security compared to that of in the local level. MANET applications considered in this study are the application in the local level, such as home networks, military applications that maintain a constant information network among soldiers, vehicles and headquarter information, and finally, a collaborative work that includes the office environment.

If the MANET is deployed in a home network, the security requirement in this scenario will be low. In this application, the routing process is accompanied to a low-level of trust and low computational cost. The establishment of MANET in a collaborative environment (business environment), need for cooperation among various users are essential to exchange information. The routing in this application should be accompanied over a medium-level of trust. Obviously, military-based applications require a high-level of security during routing. It involves a high computational cost. The various levels of trust computation are not restricted to only these applications. In this study, a fully distributed application context-aware trust based security model is presented. The proposed trust based security model decides the trust-level of geographic routing protocol based on the application context. It divides the trust-level into low, medium and high to provide security based on the application context. The aim and objectives of study are to design unified trust architecture for the MANET based on POR routing protocol. The trust management strategy deals about the application specific, context specific, by knowing the aware of the condition of the participating nodes.

The commonly used reputation based trust model is watchdog and pathrater [12]. Watchdog monitors the node's activities and behavior and pathrater gather reputation values and reacts accordingly. A new notion of developing a routing protocol introduces a trust manager component based on the trust management system [3]. It determines the trust relationships among nodes in the network on observing its neighbor's behavior in the routing process through direct and indirect ways. The major drawback of this trust management approach is that it does not implement the approach. Later, it also developed a reputation system called cooperation of nodes fairness in dynamic ad hoc networks (CONFIDANT) [4]. CONFIDANT also determines the value of trust using direct and indirect monitoring. Using these observations, it detects the malicious nodes. CONFIDANT additionally introduces an incentive scheme to reward the genuine nodes that cooperate in the routing process.

In [13], a context aware technique detects the selfish nodes. Dynamic Source Routing (DSR) is extended based on a context aware approach to punish the non-cooperating nodes. It also discards the unwanted route information to reduce the attack probability. It exploits un-keyed hash functions to identify the malicious nodes. This approach uses an inference scheme to rate the accuse level of the node. This rating prevents further service by the accused nodes. The source node uses digital signatures to broadcast the information about the detected malicious nodes. The use of digital signatures is not feasible in the resource constraint MANET. The commonly used Ad hoc on demand Distance Vector (AODV) is extended with a trust model called Trusted AODV (TAODV) [11]. AODV deploys the trust model to maintain the node's routing activities in the network. TAODV establishes the trust value among the nodes in the form of opinions. The opinions are subjective and dynamic in nature. The opinion of one node over the other may increase positively for normal communications. The opinion may decrease with their malicious activities. It involves in exchange of trust recommendations among the nodes. TAODV reduces the computation overhead by avoiding the node's request and certificate verification.

A secure routing protocol was proposed to discover malicious nodes for free end-to-end routes [7].This protocol detects the colluding

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attackers effectively. It also suggested a framework that computes and distributes the trust-value without the aid of trusted routing protocol. A secure routing protocol (SRP) is enhanced with Quality of Service (QoS) and forms a trustworthiness based Quality of Service (TQoS) routing protocol [18]. It enables a secure route set up with the addition of TQoS routing metrics. The messages involved in routing are secured with public and shared keys. It particularly detects internal attacks in routing. The work in [14], evaluates and compares the performance of a set of trust based reactive protocols. A trust architecture that enhances the reliability of a packet forwarding process in the presence of malicious nodes was presented in [19]. It is mainly based on the formation of opinion from first and second hand information. A trust framework in [10] computes trust among the nodes subjectively. It is based on the watchdog mechanism. A formal trust model is based on the information obtained from the Global Computing (GC) environment [6]. An approach in [9] collects the basic requirements for developing a trust model in ubiquitous and ad hoc networking.

A decentralized security management system evaluates trust value derived from the human notion [5]. A hybrid secured system [16] for ad hoc network, involves in both chained authentication and distributed authentication. If a node cannot determine the trust-level of its neighbor using the distributed authentication, it uses chained authentication. Trust Enhanced security Architecture for MANET (TEAM) is a unified architecture that exploits the benefit of the installed security architecture [1]. The trust model of TEAM comprises of key management mechanisms and cooperation model. An agent based trust and the reputation management (ATRM) approach exploits a clustered sensor network as supporting architecture [2].

2. CONTEXT-AWARE MULTI-LEVEL TRUST METHOD

The proposed research work has proposed application context to decide the level of trust in routing. Designing security protocols for civilian MANET is differing from the military. Trust as the confidence level that any participating entity is capable of carrying out reliably, and securely. Hence, the levels of trust requirement differ from one application to another depending on the contexts. In an application dependent context, trust is the measurable and quantifiable component of an entity regarding sincerity, security, completeness and reliability of a trustee in a context aware application. The trust-value of a node is calculated to select the trusted Next-Hop in POR.

2.1 Trusted Next-Hop Selection in POR

Now-a-days, POR is commonly applied in MANET and sensor networks. POR selects the Next-Hop using greedy forwarding approach for data forwarding. In greedy forwarding approach, the source node selects Next-Hop within its transmission range such that it is close to the destination and far away from it. POR is susceptible to different levels of attacks with respect to their impacts on routing. The common attacks are location falsifying attacks, packet dropping and misrouting attacks. This approach includes the multi-level trust model in the execution of POR. A node initially selects its neighbor list for selecting a Next-Hop. The multi-level trust model enables POR to select highly trusted Next-Hop to avoid routing attacks.

2.2 Multi-level Trust Model

The complexity of trust computation keeps on increasing with security levels. For instance, a high security level may involve complex trust computations. Trust computations consider three factors such as experience, recommendation and knowledge. A node gains experience on directly observing its neighbors and keeps on updating the trust table at regular intervals. The next level of trust computation involves in the propagation of existing trust value to the trustor as a recommendation in addition to its own direct observation. The previously evaluated trust is integrated with the knowledge factor over a regular interval, thus improving the trust computational complexity.

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

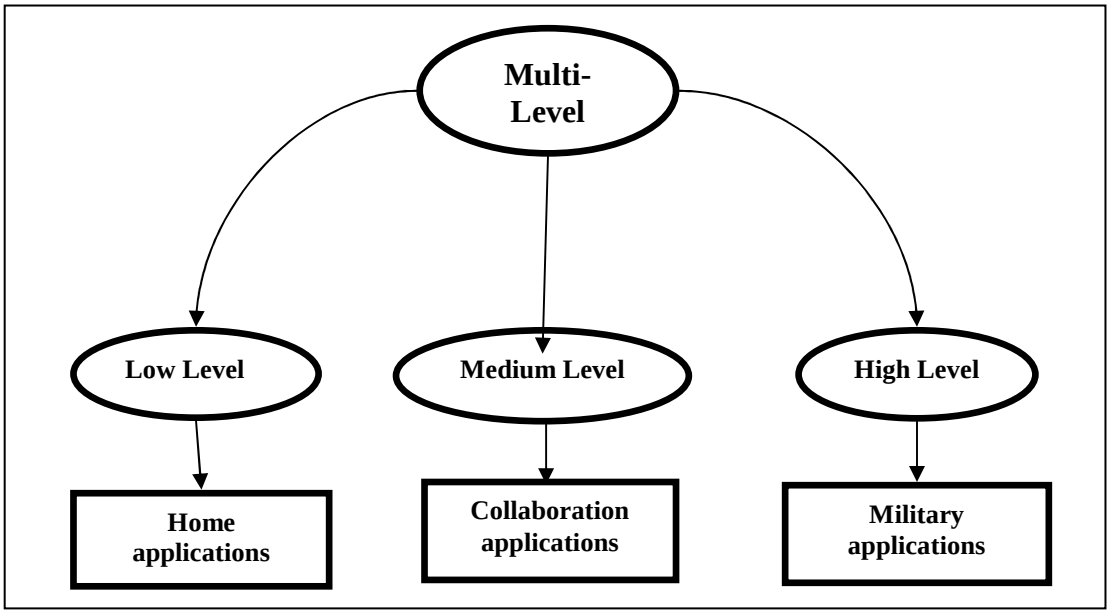

Figure 1: Multi-Level Trust Models For Security Services

The variations in the trust computational complexity satisfy various security requirements at various levels. This work focus on distributed trust computation approaches rather than centralized approaches. The POR protocol can be designed with different trust based security levels such as, Low, Medium and High, and it is application-context dependent as shown in Figure 1. The proposed trust based security model is integrated in the routing of POR that enables POR in selecting highly trusted Next Hop. The POR protocol is vulnerable to routing attacks. Therefore, this study presents multi-level trust model for POR by selecting highly trusted Next-Hop in routing.

2.3 Representation of a multi-level trust model for security

To detect routing attacks, a fully distributed trust based security model is presented as shown in the Figure 2. Various trust-levels and network metrics are listed out in the table 1. If the security level is low, it is enough to calculate the trust value of a node through direct observations. The medium-level of trust model is used where the medium security level is required. The medium-level of security may be satisfied with the recommendation based approaches in addition to direct observations. The medium-level trust model should be able to satisfy the low-level security requirements also. The high-level security environment deploys high-level trust model as it has a high probability of attacking scenarios. The high-level trust model considers the reputation value in addition to recommendation and direct observations.

Table 1: Multi-level trust models, computations and applications

Security	Trust level	Functional units	Computation cost	Overhead	applications
Low	Low	Direct observation	Low	Low	Local level (Home networks)
Medium	Medium	Direct observation+ recommendation	Medium	Medium	Collaborative work (Office environment)
High	High	Direct observation+ recommendation reputation (second hand opinions)	High	High	Military applications

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

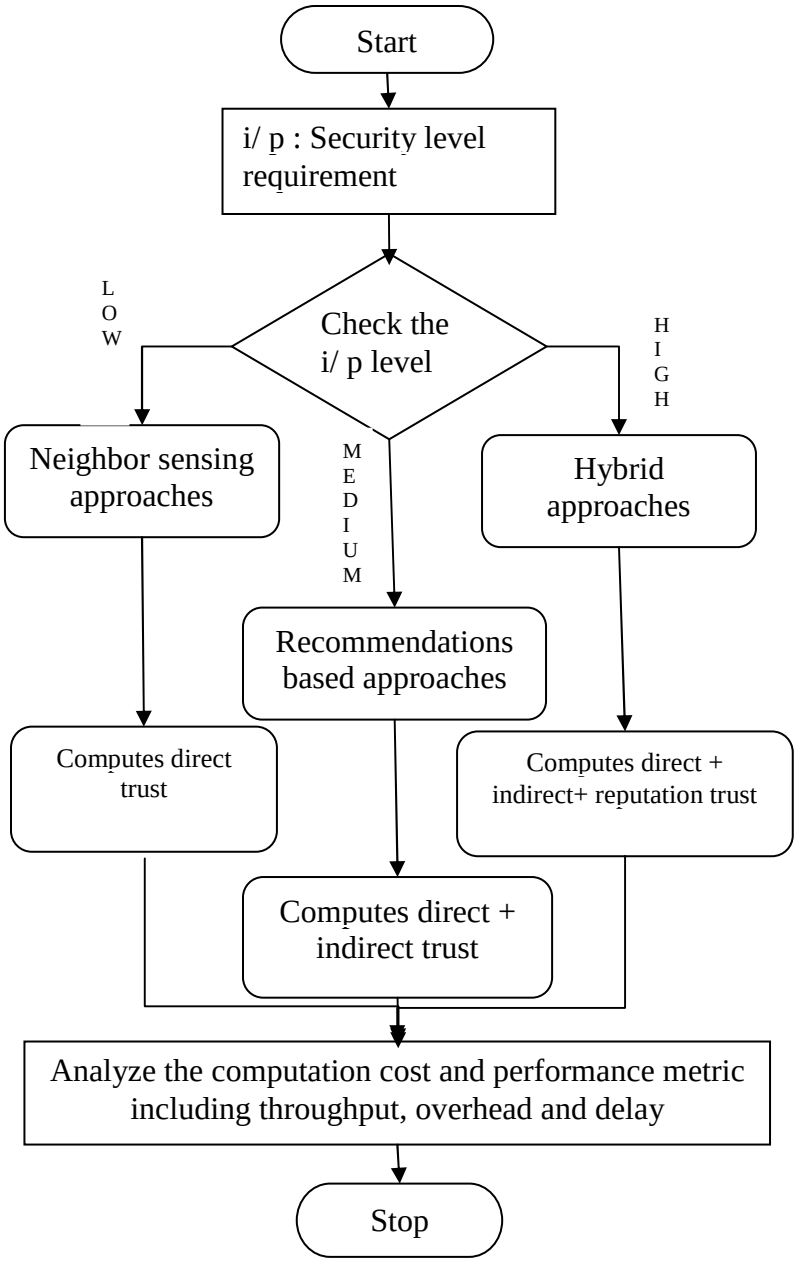

Figure 2: Computation Flow Of Multi-Level Trust Model

2.4 Low-Level trust model

This model provides only the basic security services. It must be implemented to any system by default. This trust model is modeled with low computation cost and low level security. This trust model is used in energy constraint environments. This trust model provides security in low-level. Since trust computation process does not involve much complexity, the computational cost will be low. Distributed trust computation based on neighbor monitoring provides security in a basic level with minimized computational cost. In neighbor monitoring based trust computation, each node observes its neighbor for every event occurrence, and stores its behavioral report in its cache. Each node compares its own monitored detail on an event occurrence with the monitored detail it received from the trustee node, and also from its immediate neighbors. In the direct

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

observation based trust computation, a node computes trust based on the degree of deviations among the observation it received from its neighbors.

Every node calculates the trust value of its neighbors by analyzing their behaviors. For instance, in Figure 3, node A monitors the behavior of node B through direct interactions and computes the direct trust value. For every new event, node A monitors the behavior of node B and adds the monitored behavior to its local monitoring record cache. Observations in the cache may change over time based on the behavior observed. The evaluation is performed on the basis of packet forwarding strategy if both are direct neighbors. Here, 'Node A' is Trust Evaluator or Trustor and 'Node B' is Trustee. Trust Evaluator sends 'N' packets to Trustee for the forwarding action to Destination. Now, Trust Evaluator observes the behavior of Trustee and assesses the following statistics. Initially, node A decides B's trust level based on the packet forwarding result.

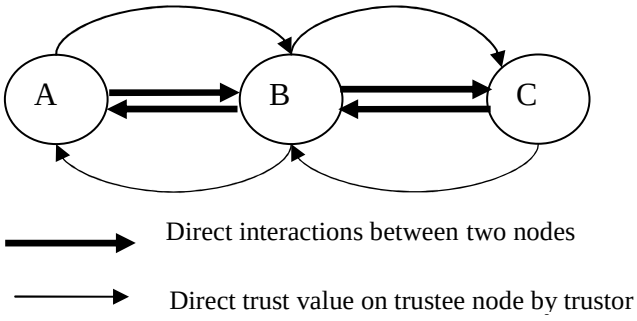

Figure 3: Neighbor node monitoring for low-level trust computation

Packet Forwarding Result = $FR_P = \{[Pf\text{-}Pd\text{-}Pi\text{-}Pm] / [Ps - Pc]\}$

Ps-The number of packets sent by trust evaluator

Pf-The number of packets forwarded by the trustee

Pc-The number of packets dropped by the trustee as a result of congestion

Pd-The number of packets delayed by trustee

Pi-The number of anonymously injected packets

Pm-The number of packets misrouted The techniques that use direct observations to detect the misbehaving nodes may fail to detect attacks due to the following reasons ambiguous collisions, and receiver collisions. In ambiguous collision, a node is prevented from overhearing its neighbor's activities. In receiver collision, a node can ensure that its neighbor has forwarded the packet, but it cannot ensure whether the third node received it. In the limited transmission power problem, a forwarding node limits its transmission power so that its transmission can be overheard by the sender but not by the receiver. To solve these problems, a common honest observer is used to assist the trust calculation. A common honest observer (h_o) is the common neighbor of nodes involved in direct observations over the geographic routing and its range is limited to a path length of 3. 'h_o' observes the behavior of nodes involved in direct observation and report to the trustor node. The report has the value of 0 or -1. These problems of direct observations have direct impact on the value of FR_P. Based on the report provided by the 'h_o', the value of FR_P changes. The FR_P value remains unchanged if it provides a positive report, i.e. h_o= 0. On the other hand, the FR_P value reduces to half if it provides a

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

negative report, i.e. h_o = -1. The modified value of FR_P is represented as $[FR_P]_m$ and given by:

$$T_L = [FR_P]_m = \begin{cases} FR_P & ; \text{if } h_o = 0 \\ FR_P/2 & ; \text{if } h_o = -1 \end{cases} \quad (2)$$

T_L is the resultant value of the low-level trust evaluation. If the value of T_L is greater than the threshold value, trustee is marked as trusted Next-Hop in the path of geographic routing. Otherwise, it is considered as malicious node. On detecting the malicious node, the trustor selects alternative node as trusted Next-Hop. The threshold value for detecting low-level attack δ= 0.4.

2.5 Medium-Level Trust Model

Medium-level trust model is used when a medium level of security is required. The computational cost for trust computation is medium. It initially computes the trust based on direct observations. The direct and indirect trust computation satisfies the medium security requirements. The trust relationship among nodes can be computed indirectly using the recommendation factor. A trust computation technique that depends on local voting is suggested in [8]. A trust network graph G is created in which it connects a node with another node, if the distance between them is one hop distance. If node B is the target node for trust computation, node A collects the belief values on B from B's neighbors and aggregates, resulting in a single trust value.

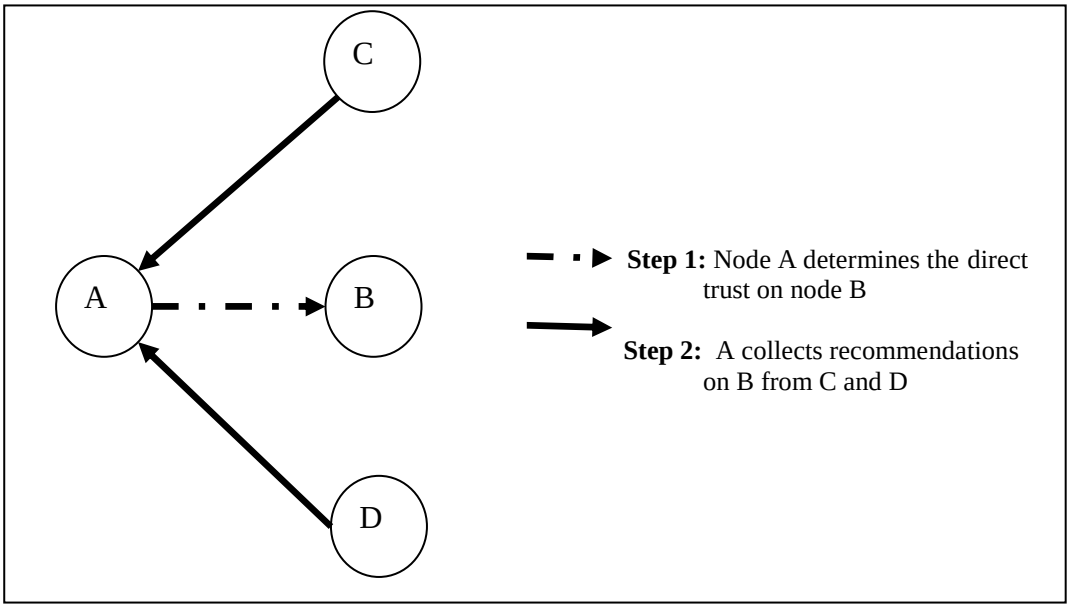

Figure 4: Direct And Indirect Trust Computation For Medium-Level Trust Model

$$T_M = \frac{\left(([FR_P]_m)_{A/B}\right) + \left(Rec([FR_P]_m)_{C/B}\right) + \left(Rec([FR_P]_m)_{D/B}\right)}{\text{The number of Recommenders} + 1} \quad (3)$$

In Figure 4, node A aggregates the recommendations obtained from nodes C and D about node B. The effective direct observation of node A on node B ($([FR_P]_m)_{A/B}$) is derived from equations (1) and (2). In this case, node C and D act as recommenders. To provide recommendations on node B, node C and D should have direct observations on B. Therefore, ($([FR_P]_m)_{C/B}$) and ($([FR_P]_m)_{D/B}$) may be calculated by following the procedures in equations (1) and (2). The node C and D forwards the value of direct observation as recommendations to node A using Recommendation Exchange Protocol (REP) and represented as ($Rec([FR_P]_m)_{C/B}$) and ($Rec([FR_P]_m)_{D/B}$).

In REP, recommendations are only exchanged among the neighbors [15]. It minimizes

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the recommendation error probability as it involves processing of only smaller number of the recommendations. Moreover, a node may compare the received recommendations with its own observations to compute the trust-level. This comparison is accurate as nodes compute the trust-level of neighboring nodes such that it has previous knowledge about them. REP uses a minimum number of messages that reduce both network traffic and energy consumption.

The messages are transmitted to only the neighbor i.e. one hop away. Thus, avoiding flooding in multi-hop communication. REP consists of three message types, Trust Request (T_{REQ}), Trust Reply (T_{REP}), and Trust Advertisement (T_A). If two nodes contact for the first time, each transmits T_{REQ} message to the other node. The node that has trustee as a neighbor, sends back the reply message, T_{REP} in which it has the recommendation about the trustee. In order to avoid collisions, reply message is sent after waiting for a period, T_{WAIT}, and it waits for receiving T_{REQ} messages from other nodes.

The major problem with the recommendation based approach is that the recommender may be a dishonest node. The trustor should check for it before considering the recommendation values. The trustor node A compares its own direct observation on B with the recommendations received from C and D. If A's direct observation coincides with the received recommendations, the recommender is an honest node otherwise it is a dishonest node.

In the equation (3), the recommended values and direct observation value are aggregated to effectively judge the state of the recommender and trustee. In case, if trustee is a malicious node, it may behave in good manner to trustor and not to the recommenders. Therefore, there is a chance for trustor to mark recommenders as malicious. To avoid this false judgment, all the trust values are aggregated with respect to its own observation value and the values obtained from the total number of recommenders. This trust model prevents the routing from medium-level attacks. To meet the medium level of security requirements, the level of threshold value is increased. If the value of T_M is greater than the threshold value,δ, trustee is considered as trusted Next-Hop in the geographic routing. The threshold value for a medium-level trust model δ= 0.50.

2.6 High-Level Trust Model

This level of trust is preferred in a military environment. The high-level trust model has more computing complexity and also provides a strong security level. The direct, indirect and reputation scheme satisfies the high level security requirements. As it involves direct and indirect observations on node behavior, it can be referred as hybrid approach. This trust model is required only if there is a "high" requirement of security. This trust model has resulted in high computational cost. The high-level trust model also satisfies the requirement of both low and medium-level trust models. The complexity in designing the high secured trust model is extremely high. Several factors must be considered during the trust model designing. Though it has high computational cost, the packet delivery rate and throughput is high as the system is highly secured. In the hybrid approach, trust of a node can be evaluated based on direct experience, recommendations and reputations as shown in Figure 5.

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

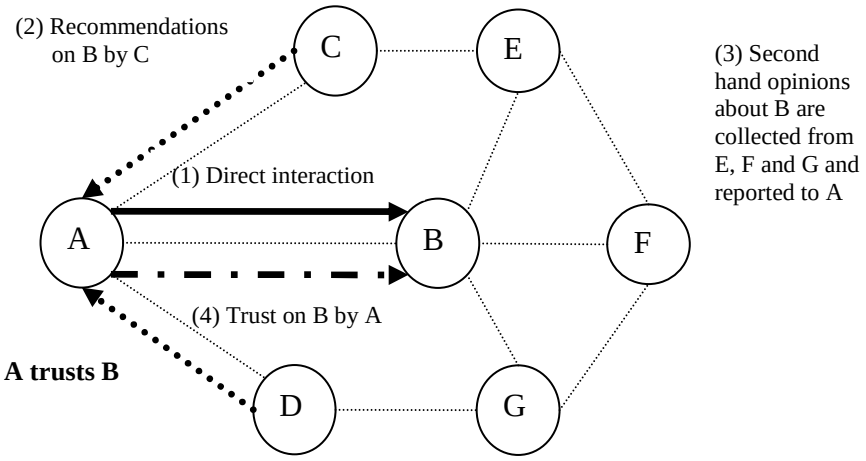

Figure 5: Hybrid approach for high-level trust computation

The trust computation technique based on a linear grouping is self-evaluated trust and trust evaluated by other nodes (neighbors) ($0 \leq T_M \leq 1$) for MANET as in the equation (3). In addition, second hand opinions are also collected on the trustee. The second hand opinion is formed not only considering the past behavior. However, it also considers the behavior of trustee over a period. The reputation value helps in making accurate decisions as the second hand opinions are not measured instantaneously. The high-level trust value of node B calculated by node A is given by $T_{H.}$

$$T_H = \alpha T_M + T_{r\,(B/A)} \quad (4)$$

In equation (4), T_r is the trust value calculated using reputation values. The reputation values are gathered by considering nodes as reputation requestors and reputation suppliers. It compares the reputation results to the results gained from direct observations and recommendation results.

The reputations are second hand opinions obtained from the non- immediate one hop neighbors of the trustor nodes. In the Figure 5, the second hand opinion of trustee node B is collected from nodes E, F and G. The second hand opinion is represented as TSH. The second hand opinions are aggregated and forwarded to node A.

$$T_{r\,(B/A)} = TSH_{E \to B} + TSH_{F \to B} + TSH_{G \to B} \quad (5)$$

$T_{r\ (B/A)}$ is aggregated using Weighted average technique. In Weighted average technique, the Weighted average of weighted trust evaluation by all neighboring nodes on node B is taken as the value of $T_{r\ (B/A)}$. Every node retains a trust table containing details about each of its neighbors. In the trust table, values are recorded for a number of events. The trustor evaluates the trust-level based on the security requirement and values in the trust table. This high-level trust model can detect the attacks like wormhole, a black hole and Denial of Service (DoS). Malicious nodes can be detected if the computed trust-level drops below a threshold value. The range of threshold value should be higher than that of the medium-level trust model. The high-level trust model has a threshold value of 0.80. The evaluated trust value is then included in the routing function to ensure that it forwards the message only to the trusted node, thus provides security in routing.

3. RESULTS

To evaluate the performance of the multi-level trust model with POR, the critical environment is simulated by varying the attacker fraction using the Network Simulator (NS- 2). Network under the routing protocol POR without trust and with the trust model is simulated for the comparative analysis in the presence of attackers. The nodes are deployed randomly in the square region of size 2500m X 2500m. The nodes follow a random way point mobility model with the pause time of 25 sec and the speed of 10 m/s. Performance of the proposed trust model is experimented in the network consists of various proportion of attacker nodes are considered. Low, Medium and a high-level trust model consists of a maximum of 25, 75, and 125 attacker nodes

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

respectively. Each node is capable of 150m transmission range. Simulation is performed at the Traffic rate of 512bytes/sec with 60 CBR flows. Since the trust is evaluated in three levels based on the application context, the comparative performance of trust against the POR without trust is evaluated.

Table 2: Simulation Parameters Of The Multi-Level Trust Model

Parameter	Values
Total Number of Nodes	500
Network Area	2500m X 2500m
Size of Packet	512 bytes
Mac Type	802.11
Routing Protocol	POR
Transport Agent	UDP
Application Agent	CBR
speed	10m/s
Mobility model	Random Way Point
Transmission Range	150m
Simulation Time	500seconds

Table 2 illustrates the Simulation Parameters of the multi-level trust model. Packet Delivery Ratio (PDR), overhead, and average end-to-end delay, are considered as the performance metrics to evaluate the effectiveness of the multi-level trust model. Evaluate these metrics by varying the attacker fraction to prove the effectiveness of the proposed trust model in the dynamic MANET environment.

3.1 Attacker Model For Simulation:

The MANET nodes communicate with each other through a restricted bandwidth and error prone wireless medium. These features of MANET motivate the attackers to launch several attacks on the network. The trust management system plays a major role in decision making, and hence, it has become an attractive target for adversaries. This work considers the network as a directed graph G (V, E) in which V represents the participating nodes and E represents the trust relationship links. The graph G is termed as the "Trust Graph". The modeled trust graph is different from the physical graph. Assume that 'n' represents the total number of nodes in the network and hence, |V|= n. Therefore, each node in the network is labeled with indices V= {1,2,3… n}. This work does not depend on any centralized entity. On the other hand, the nodes in the network compute the trustworthiness of other nodes based on their previous communications and second hand information. For instance, the node 'A' can rate the trustworthiness of node 'B' after requesting some files based on the response made by node 'B'. The direct link between node A and B in graph G is represented as (A→B), and it also represent the direct trust relation. If any two nodes in the network have no contacts i.e. (A→B)∉ E, the trust value between them is uncertain. Let T represent the trust rating of one node on another node and trust relations are asymmetric i.e. $T_{(A\rightarrow B)} \neq T_{(B\rightarrow A)}$. This work considers three levels of attacks and corresponding trust models. The threshold value for low level, medium level and high level attacks are represented as δ_L, δ_M, and δ_H respectively. If any of the node in the network has less than the corresponding threshold value, it is considered as an attacker. For simulation purpose, this work assumes attackers of 5%, 15% and 25 % of 'n' in the low, medium and high-level trust model respectively.

Let n_L, n_M and n_H represent the number of attackers in the low, medium and high-level trust model. The attackers have the ability to rate the genuine node as "bad" and malicious as "good". The attackers can improve their T value by genuinely participating in the routing. On the other hand, if the attackers continue to show signs of constant malicious behavior, the trust model eliminates the attacker from the network. The performance of proposed trust model is evaluated using the parameter called attack fraction. The relation between attacker fraction and number of attackers in each model is shown in table 3.

Table 3: Number Of Attacker Nodes In Each Model

Attacker fraction	Attacker nodes in low-level trust model	Attacker nodes in medium-level trust model	Attacker nodes in high-level trust model	Total number nodes
0.2	5	15	25	500
0.4	10	30	50	500
0.6	15	45	75	500
0.8	20	60	100	500
1	25	75	125	500

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2 Performance Analysis

This section explains the performance valuation of the proposed scheme and compares with POR. This section also compares the performances among the proposed multi-level trust models.

3.2.1 Packet delivery ratio

In sub section of Figure 6 shows the performance of the multi-level trust model and the effect of the packet delivery ratio with respect to various attacker fraction scenarios. Figure 6a shows the PDR of low-level trust model. POR with a low-level trust model achieves a higher packet delivery ratio than the simple POR. However, increment in the proportion of attackers decreases the packet delivery ratio in both the cases. The Figure 6b shows the effect of the PDR for medium-level trust model. The medium trust model involves the trust evaluation mechanism that prevents the medium and low-level attacks in the routing path. Therefore, the medium-level trust model provides better PDR compared to simple POR. The Figure 6c shows the effect of PDR for high-level trust model. POR with a high-level trust model detects all kind of attacks from low-level to high-level. This feature greatly reduces the packet failures in the network and achieves higher PDR in the network compared to simple POR. The Figure 6d depicts the effect of the PDR for various attacker fraction scenarios. Gradual increment of attacker proportion in the network affects the process of packet delivery by invoking various attacks over the network.

POR with a high-level trust model achieves a superior PDR compared to other levels of trust model. This is due to the sophisticated computation of trust, and it includes the functionality of low and medium-level trust computation in order to select the most trusted next hop. Consequently a high-level trust model protects the network from all kinds of threat imposed by the attacker.

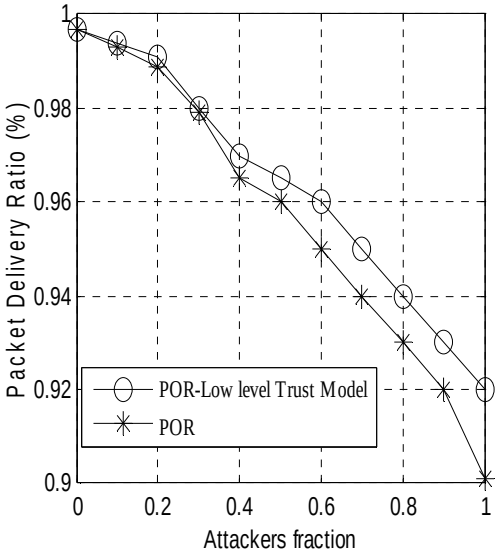

Figure 6a: Packet Delivery Ratio Of Low-Level Trust Model

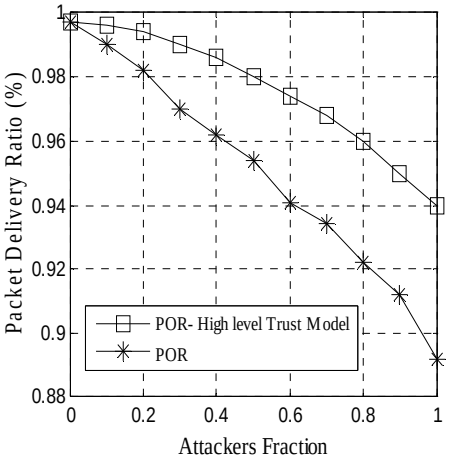

Figure 6c: Packet Delivery Ratio Of High- Level Trust Model

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

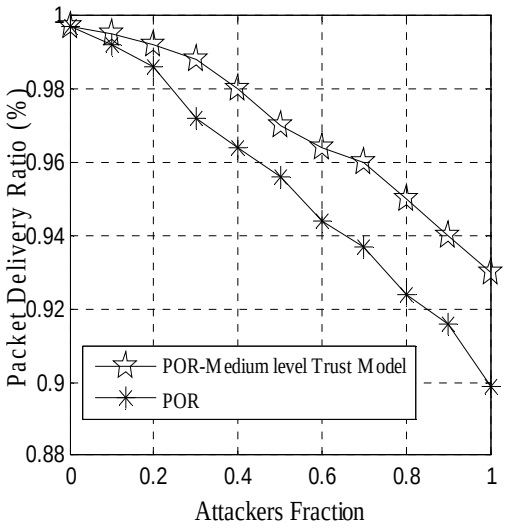

Figure 6b: Packet Delivery Ratio Of Medium-Level Trust Model

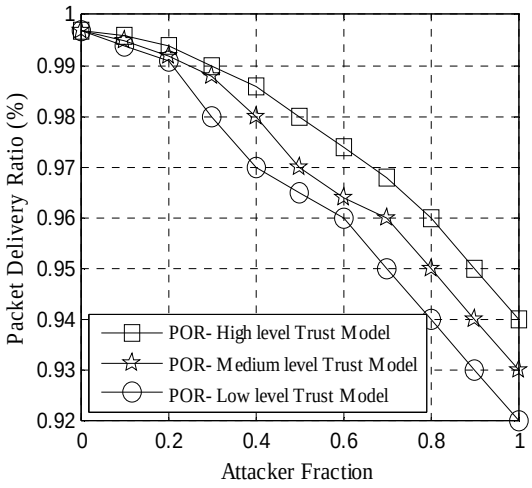

Figure 6d: Comparative Analysis Of Packet Delivery Ratio Of Low, Medium And High- Level Trust Models

Figure 6: Illustration Packet Delivery Ratio Parameter

3.2.1 Overhead

In sub section of Figure 7 shows the effect of overhead of the multi-level trust model with respect to various attacker fraction scenarios. A low-level trust model involves the packet forwarding analysis which invokes a specific overhead in the network during the direct observation process. Fig 7a shows the overhead of the low-level trust model. Report from the common honest observer is invoked for accurate calculation of trust and hence, increases the overhead in the network. Thus, Overhead in POR with a low-level trust model is increased compared to simple POR. The Figure 7b shows the effect of overhead for the medium-level trust model with respect to various attacker fraction scenarios. In addition to overhead incurred during direct observation, control messages involved in REP protocol involved in the medium-level trust model invokes the significant overhead in the network. Therefore, medium-level trust model results in a higher overhead in the network compared to low-level trust model. Since the objective of this trust model is to facilitate the highly secure routing, high computation is required. From the Figure 7c, it is clear that, high computational complexity invokes a significant amount of overhead in the network. Overhead is much higher while using a high-level trust model than simple POR. The reason is the involvement of the number of functionalities such as direct observation, the recommendation exchange using REP protocol, and reputation from non immediate one hop neighbors. The Figure 7d illustrates the overhead caused in the network with respect to different trust level computations under different mobility conditions. Therefore, overhead increases when the attacker fraction is increased. Since the complexity of computation is progressively increased as the level of trust computation increases, overhead also increases in each level. POR with a high-level trust model invokes much overhead in the network compared to other levels. Even though the overhead is high, it achieves the highest trust among other levels with the trade off of overhead.

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

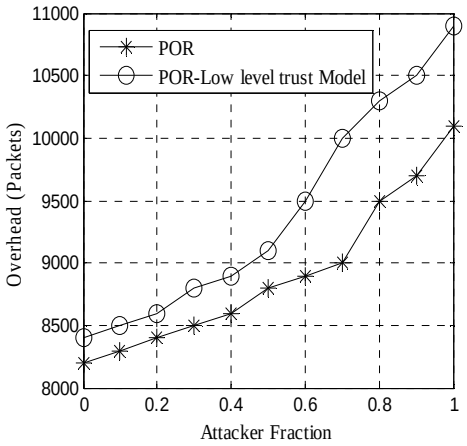

Figure 7a: Overhead of low-level trust model

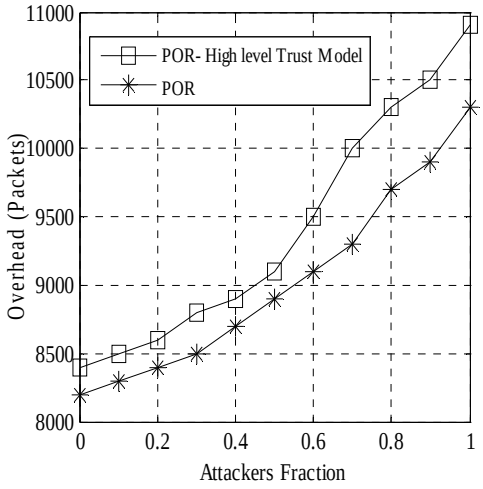

Figure 7c: Overhead of high-level trust model

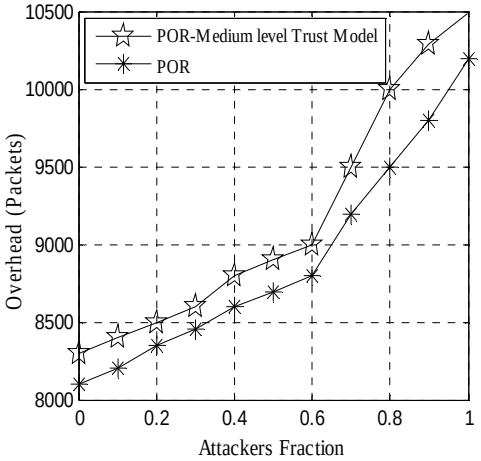

Figure 7b: Overhead of medium-level trust model

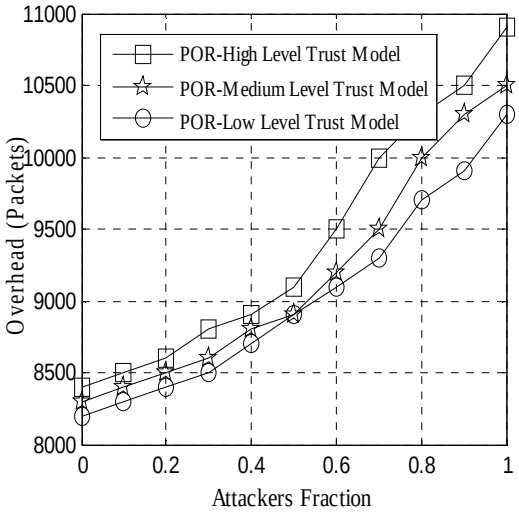

Figure 7d: Comparative analysis of overhead of low, medium and high-level trust models

Figure 7: Illustration of overhead parameter

3.2.2 Average End To End Delay

In sub section of Figure 8 shows the effect of the average end-to-end delay of multi-level trust with respect to various attacker fraction scenarios. The high computation carried out by the trust model causing the delay in the network. In simple POR next hop is selected on the basis of greedy forwarding technique. However, in a low-level trust model, computation is performed with direct observation and report from a common honest observer. Next hop is selected only based on the result of computation increases the average end to end delay in the network compared to simple POR. On the other hand, POR with a low-level trust model ensures the data delivery over the trusted path with some delay as depicted in Figure 8a. The Figure 8b shows the effect of average end-to-end delay for medium-level trust model with respect to various attacker fractions. A considerable amount of time is incurred during the recommendation exchange process using REP protocol increases the time involved in the next hop finding process. Therefore, average end-to-end delay is higher in POR with a medium-level trust model compared to simple POR. Most sophisticated computation is carried out to provide the high secured environment which consumes time for the computation itself. Therefore, average end-to-end delay is increased in this high-level trust model as shown in the Figure 8c. In a high-level trust model, significant time is consumed for

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the evaluation of trust since more complex metrics are involved, and it is due to the involvement of the process of reputation value gathered from nodes in the network. Therefore, there exists much higher delay in the implementation of POR with a high-level trust model when compared to simple POR. The Figure 8d. shows the average end-to-end delay caused due to various trust level computation scenarios. The highly dynamic condition link breakage forces the discovery of new next-hop. Additional time is consumed for the calculation of trust for the new next-hop along with the time taken for a regular next-hop calculation process designed for a greedy forwarding process. Time required for new next-hop calculation is significantly high when the complexity of trust computation is improved. Therefore, the average end-to-end delay is increased with the trust level.

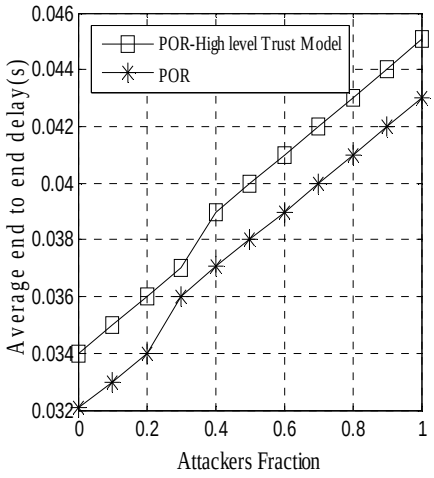

Figure 8a : Average end-to-end delay of low-level trust model

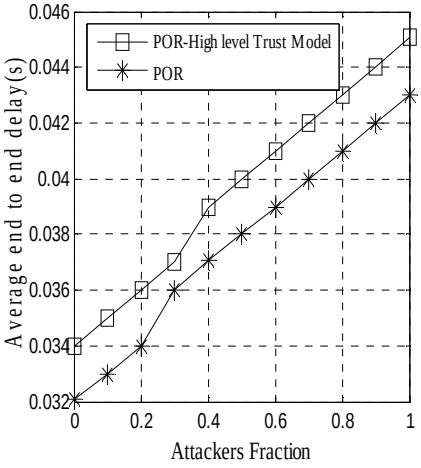

Figure 8c : Average end-to-end delay of high-level trust model

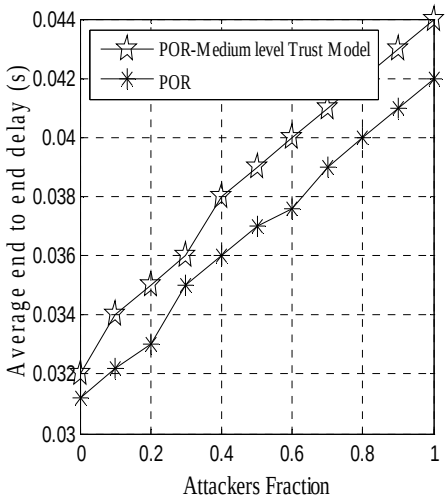

Figure 8b : Average end-to-end delay of medium-level trust model

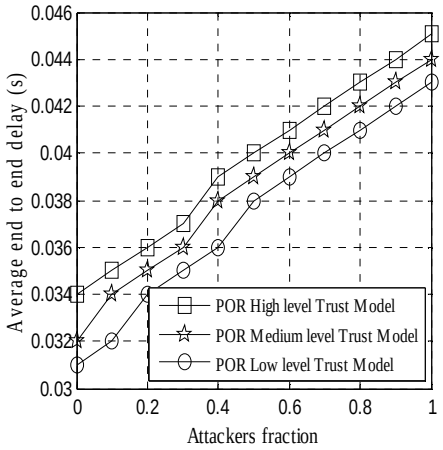

Figure 8d : Comparative analysis of average end-to-end delay of low, medium and high- level trust models

Figure 8: Illustration Of Average End-To-End Delay Parameter

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. CONCLUSION

This study proposed a multi-level trust model for MANET with geographic routing that can be applied to enhance the trust measure in the routing process. It presents an effective application context-aware trust based security model. The proposed trust architecture meets various levels of security requirements in the geographic routing, POR. The proposed work does not require exact time synchronization, complex hashing and authentication techniques. The proposed approach is fully distributed. The proposed multi-level trust model is designed in three levels based on context-aware security. Three levels of trust model include low, medium and high. Each of these levels ensures a security level that satisfies the context's security requirements. The proposed work facilitates the POR to select only the trusted node as the Next Hop, thus preventing several routing attacks. The performance of the proposed trust model is compared with the POR in the presence of attacking nodes to prove its superiority. The simulation is performed by varying the number of attackers to show the effectiveness of the proposed work. The simulation results prove that the proposed multi-level trust model prevents the network from routing attack, thus maintaining high throughput and packet delivery ratio.

REFERENCES

[1] Balakrishnan, V., V. Varadharajan, U. Tupakula and P. Lucs, 2007. "TEAM: Trust enhanced security architecture for mobile ad-hoc networks". *Proceedings of the 15th Conference on Networks*, November 19-21, 2007, Adelaide, SA., pp: 182-187.

[2] Boukerch, A., L. Xu and K. EL-Khatib, 2007. "Trust-based security for wireless ad hoc and sensor networks". *Comput. Commun*., 30: 2413–2427.

[3] Buchegger, S. and J.Y. Le Boudec, 2002a. "Nodes bearing grudges: Towards routing security, fairness and robustness in mobile ad hoc networks". *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-Based Processing*, January 2002, IEEE Computer Society, pp: 403-410.

[4] Buchegger, S. and J.Y. Le Boudec, 2002b. "Performance analysis of the CONFIDANT protocol". *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

[5] Cahill, V., E. Gray and J.M. Seigneur, C.D. Jensen and Y. Chen et al., 2003. "Using trust for secure collaboration in uncertain environments". *IEEE Pervasive Comput. Mag*., 2: 52- 61.

[6] Carbone, M., M. Nielsen and V. Sassone, 2003. "A formal model for trust in dynamic networks". *Proceedings of the 1st International Conference on Software Engineering and Formal Methods*, September 22-27, 2003, Brisbane, Queensland, Australia, pp: 54-61.

[7] Ghosh, T., N. Pissinou and K.S. Makki, 2005. "Towards designing a trusted routing solution in mobile ad hoc networks". *Mobile. Networks Applic*., 10: 985-995

[8] Jiang, T. and J.S. Baras, 2006. "Trust evaluation in anarchy: A case study on autonomous networks". *Proceedings of the 25th International Conference on Computer Communications, April 2006, Barcelona, Spain*, pp: 1-12.

[9] Lamsal, P., Yla-Jaaski, A. and T. Hasu (Eds.). Helsinki 2002. "Requirements for Modeling Trust in Ubiquitous Computing and Ad Hoc Networks. In: Ad Hoc Mobile Wireless Networks-Research Seminar on Telecommunications Software", University of Technology, Espoo

[10] Li, J., R. Li and J. Kato, 2008. "Future trust management framework for mobile ad hoc networks". *Commun. Mag*., 46: 108-114.

[11] Li, X., M.R. Lyu and J. Liu, 2004. "A trust model based routing protocol for secure ad hoc networks". *Proceedings of the IEEE Conference on Aerospace*, Volume 2, March 6-13, 2004, Big Sky, Montana, USA., pp: 1286-1295.

[12] Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. "Mitigating routing misbehavior in mobile ad hoc networks". *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, August 6-11, 2000, Boston, MA., USA., pp: 255-265.

[13] Paul, K. and D. Westhoff, 2002. "Context aware detection of selfish nodes in DSR based ad-hoc networks". *Proceedings of IEEE Global Telecommunications Conference*, August 7-9, 2002, IEEE Computer Society, Washington, DC, USA., pp: 178-182.

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14] Pirzada, A.A., C. McDonald and A. Datta, 2006. "Performance comparison of trust-based reactive routing protocols". *IEEE Trans. Mobile Comput*., 5: 695- 710.

[15] Velloso, P.B., R.P. Laufer, D. de O. Cunha, O.C.M.B. Duarte and G. Pujolle, 2010. "Trust management in mobile ad hoc networks using a scalable maturity-based model". *Trans. Network Serv. Manage.*, 7: 172-185.

[16] Wang, G., Q. Wang, J. Cao and M. Guo, 2007. "An effective trust establishment scheme for authentication in mobile ad-hoc networks". *Proceedings of the 7th International Conference on Computer and Information Technology*, October 16-19, 2007, Aizu-Wakamatsu, Fukushima, pp: 749-754.

[17] Yang, S., C.K. Yeo and B.S. Lee, 2012. "Toward reliable data delivery for highly dynamic mobile ad hoc networks". *IEEE Trans. Mobile Comput*., 11: 111-124.

[18] Yu, M. and K.K. Leung, 2009. "A trustworthiness-based qos routing protocol for wireless ad hoc networks". *Trans. Wireless Commun*., 8: 1888-1898.

[19] Zouridaki, C., B.L. Mark, M. Hejmo and R.K. Thomas, 2005." A quantitative trust establishment framework for reliable data packet delivery in MANETs". *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, November 7, 2005, ACM New York, USA., pp: 1-10.